IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Richmond Division

UNITED STATES OF AMERICA	)	
	)	
v.	)	CRIMINAL NO. 3:19-CR-130-MHL
	)	
OKELLO T. CHATRIE,	)	
	)	
Defendant.	)	

GOVERNMENT'S RESPONSE IN OPPOSITION TO DEFENDANT'S MOTION FOR SUPPRESSION OF EVIDENCE OBTAINED PURSUANT TO GOOGLE GEOFENCE WARRANT

The United States of America, by its undersigned attorneys, moves this Court to deny Defendant Okello T. Chatrie's motion to suppress evidence obtained from Google, LLC ("Google") pursuant to a search warrant for GeoFence location information (the "GeoFence warrant"). (ECF No. 29.)

The warrant authorized disclosure from Google of two hours of location information associated with electronic devices that were, within a one-hour interval, within 150 meters of the site of a bank robbery. This Court should deny the defendant's motion for three reasons. First, investigators did not conduct a search under the Fourth Amendment when they obtained this information from Google. Second, the GeoFence warrant complied with the Fourth Amendment, as it was issued based on probable cause and specified its object with particularity. Third, suppression is inappropriate because investigators relied on the warrant in good faith.

I. BACKGROUND

At approximately 4:50 p.m. eastern standard standard time, on May 20, 2019, a then-unknown male entered the Call Federal Credit Union in Midlothian, Virginia with a firearm. While the man stood in line, victim-teller J.B. asked another teller, J.W., to assist this customer

when he reached the counter. When he reached J.W.'s station, the man presented a handwritten note. That note read, in part, "I got your family as hostage and I know where you live, If you or your coworker alert the cops or anyone your family and you are going to be hurt . . . I need at least 100k." After J.W. told him that she did not have access to that amount of money, the armed robber pulled out a silver and black handgun. Waving the firearm around, he then directed J.W., other Call Federal Credit Union employees, and customers to move to the center of the lobby and get on the floor. Once there, the armed robber led victims behind the teller counter and into a back room where the Credit Union's safe was located.

Once in the back room, he ordered everyone to their knees at gunpoint and demanded that the bank manager open the safe. The Credit Union manager, fearing for his life, obliged by opening the safe and handing over $195,000 in United States currency.

After the armed robbery, victims dialed 911 to request assistance. When law enforcement arrived, they reviewed surveillance video from the credit union and determined that the armed robber entered the credit union from an area behind a nearby church, held a cellular telephone to his ear when entering the credit union, and ran back towards the church after the robbery. An employee of that church explained to law enforcement that he saw a suspicious individual in a newer model, blue Buick sedan prior to the time of the robbery.

Investigators knew that Google stored location information that could help them apprehend and convict the robber. Google obtains and stores its customers' location information for a wide variety of purposes. Google explains: "From driving directions, to making sure your search results include things near you, to showing you when a restaurant is typically busy, location can make your experiences across Google more relevant and helpful. Location information also helps with some core product functionality, like providing a website in the right language or helping to

keep Google's services secure." How Google Uses Location Information (available at https://policies.google.com/technologies/location-data).

In particular, Federal Bureau of Investigation Task Force Officer Josh Hylton knew that in response to a "GeoFence" warrant, Google could produce location and identity information from accounts associated with electronic devices present in a specified area at a specified time. In one of his previous robbery investigations, an Assistant United States Attorney had reviewed his application for a federal GeoFence search warrant, and he subsequently applied for and obtained a GeoFence warrant in that investigation from a United States Magistrate Judge. In addition, he had previously discussed GeoFence warrants with a Virginia state prosecutor, who had expressed no concerns about their constitutionality.

On June 14, 2019, Task Force Officer Hylton sought and obtained a GeoFence warrant from the Chesterfield Circuit Court of Virginia. His statement of probable cause began by describing the facts of the robbery, including that prior to the robbery, the robber held a cell phone and appeared to be speaking with someone. *See* State GeoFence Warrant at 4.[1] The statement then explained why there was reason to believe that Google would have evidence pertaining to the robbery. Among other facts, the statement disclosed: (1) that as of 2013, 56% of cell phones were smartphones; (2) that "[n]early every" Android phone "has an associated Google account"; (3) that Google "collects and retains location data" from such devices when the account owner enables Google location services; and (4) that Google collects location information from non-Android smartphones if the devices are "registered to a Google account and the user has location services enabled." *Id.* at 5. Magistrate David Bishop issued the GeoFence warrant upon a finding of

[1] The United States will provide a copy of the entire GeoFence search warrant application to the Court in conjunction with this motion.

probable cause. *Id.*

The GeoFence warrant specified a target geographical area, identified as a circle of radius 150 meters around a specific latitude and longitude point near the bank. *See id.* at 3. It authorized disclosure of location information over a two-hour interval (from 3:50 pm to 5:50 pm) from accounts associated with devices within this target area at some point during a one-hour interval that included the robbery (from 4:20 pm to 5:20 pm). *See id.* at 2-3. The warrant also authorized disclosure of specified customer identity information associated with these accounts, including user name and email address. *See id.* at 3.

The warrant authorized this disclosure through a three-step process that enabled law enforcement to "narrow down" the information disclosed by Google and thus obtain less than the maximum amount of information covered by the warrant. *Id.* at 2-3. The warrant directed that in the first step, Google was to disclose location information for devices present in the target area during the hour of the robbery, but not the identity information associated with the devices. *See id.* at 2. In the second step, law enforcement was to review the anonymized location information produced by Google and identify the accounts of interest, and Google was then to disclose location information for those accounts over the full two-hour interval, both within and outside of the target area, but again without disclosing identity information. *See id.* at 2-3. In the third step, law enforcement was to identify accounts that remained of interest, and Google was to disclose subscriber identity information for those accounts. *See id.* at 3.

Investigators followed this three-step process when they executed the warrant. In step one, Google produced one hour of location information within the target area for 19 anonymized accounts. In step two, investigators identified nine of those accounts for further disclosure, and Google produced two hours of anonymized location information for those nine accounts. The

anonymized information showed one account of particular interest (hereinafter, the "Chatrie Account"), as it was associated with a device that: (1) was near the church prior to the robbery at the same time that the church witness recalled seeing the suspicious individual; (2) inside the credit union during the robbery; and (3) immediately left the area following the robbery via the area near the church. In step three, law enforcement requested and obtained subscriber information for three accounts, including the Chatrie Account, which belonged to the defendant. This information included the defendant's email address and that he used an Android phone and Google Location History.

As the owner of an Android phone, the defendant had affirmatively opted-in to Google's use and storage of his location information. *See* Google Privacy Policy (available at https://policies.google.com/privacy/archive/20190122) ("You can also turn on Location History if you want to create a private map of where you go with your signed-in devices.").[2] He also had the ability to delete his location history. *See id.* In addition, he agreed to disclose his location information to Google for multiple purposes, including for Google to provide "personalized" services to him (including "content and ads" or "driving directions") and for Google to develop new services. *See id.*

Subsequent investigation provided further evidence that the defendant was the robber. On September 17, 2019, the grand jury returned a two-count Indictment for Forced Accompaniment during an Armed Credit Union Robbery, in violation of 18 U.S.C. § 2113(e), and Brandishing a Firearm During and in Relation to a Crime of Violence, in violation of 18 U.S.C. § 924(c)(1)(A)(i).

[2] Google archives changes over time to its Privacy Policy. *See* https://policies.google.com/privacy/archive. Here, the United States references the Privacy Policy that was in effect from January 22 to October 14, 2019, a period which includes the bank robbery.

The defendant pleaded not guilty on October 1, 2019, and trial was scheduled for December 3, 2019, through December 5, 2019, at 9:00 a.m. before the Honorable M. Hannah Lauck.

On October 29, 2019, the defendant filed the Motion to Suppress that is subject of this response.

II. ARGUMENT

A. The Defendant Had No Reasonable Expectation of Privacy in Two Hours of Google Location Information

As set forth below, the defendant had no reasonable expectation of privacy in any of the information disclosed by Google pursuant to the GeoFence warrant. The defendant argues that he had a reasonable expectation of privacy in his location information under *Carpenter v. United States*, 138 S. Ct. 2206 (2018), but *Carpenter* held only that the government infringes a cell phone owner's reasonable expectation of privacy when it accesses seven days or more of cell phone location information. *See Carpenter*, 138 S. Ct. at 2217 n.3. Here, the United States' acquisition of two hours of the defendant's location information is governed by the long-standing principle that a person has no reasonable expectation of privacy in information disclosed to a third party and then conveyed by the third party to the government.[3]

1. Obtaining Two Hours of the Defendant's Location Information Was Not a Search Under *Carpenter*

The defendant claims based on *Carpenter* that he had a reasonable expectation of privacy in the two hours of location information disclosed by Google, but *Carpenter* does not bear the weight he places on it. In *Carpenter*, the Supreme Court determined that individuals have a

[3] Google also disclosed to the government the defendant's basic subscriber information, including email address, Google Account ID, and Google services used. In *United States v. Bynum*, 604 F.3d 161, 164 (4th Cir. 2010), the Fourth Circuit held that a subscriber has no reasonable expectation of privacy in such information. The defendant does not claim any protected privacy interest in this information.

"reasonable expectation of privacy in the whole of their physical movements," and it held "that accessing seven days of [cell-site location information] constitutes a Fourth Amendment search." *Carpenter*, 138 S. Ct. at 2217 & n.3.

The Court emphasized that its decision was "a narrow one." *Carpenter*, 138 S. Ct. at 2220. It explicitly declined to determine whether there is a "limited period" for which the government can acquire cell phone location information without implicating the Fourth Amendment. *Id.* at 2217 n.3. It also explicitly refused to decide whether obtaining a cell tower dump constituted a Fourth Amendment search. *See id.* at 2220. This limitation is relevant here because tower dump information is similar to the information disclosed pursuant to the GeoFence warrant. A tower dump includes "information on all the devices that connected to a particular cell site during a particular interval." *Id.* Here, the GeoFence warrant sought information on all devices that were within a particular area during a particular interval.

Although *Carpenter* declined to resolve whether obtaining two hours of cell phone location information constitutes a search, *Carpenter*'s reasoning suggests it does not, because *Carpenter* is focused on protecting a privacy interest in long-term, comprehensive location information. The Court began its opinion by framing the question before it as "whether the Government conducts a search under the Fourth Amendment when it accesses historical cell phone records that provide a comprehensive chronicle of the user's past movements." *Carpenter*, 138 S. Ct. at 2212. The Court emphasized that long-term cell-site information created a "comprehensive record of the person's movements" that was "detailed" and "encyclopedic." *Id.* at 2216–17. It explained that "this case is not about 'using a phone' or a person's movement at a particular time. Rather, the Court explained, the case concerned a detailed chronicle of a person's physical presence compiled every day, every moment, over several years." *Id.* at 2220. By this standard, the government did not

conduct a search when it obtained the defendant's location information pursuant to the GeoFence warrant.

Two hours of location data is only 1/84th of the period that *Carpenter* held constituted a search, and it does not provide the sort of "all-encompassing record of the holder's whereabouts" and "intimate window into a person's life" that concerned the Court. *Carpenter*, 138 S. Ct. at 2217. Rather than providing an encyclopedic chronicle of the defendant's life, the information disclosed by Google provided a summary of his location for less than half an afternoon. This information is not quantitatively or qualitatively different from information that could be obtained from other sources, such as surveillance video or live witnesses.

The United States is not aware of any judicial opinions addressing whether a GeoFence warrant infringes a reasonable expectation of privacy under *Carpenter*. The Seventh Circuit, however, held that *Carpenter* "does not help" a robber identified via tower dumps. *United States v. Adkinson*, 916 F.3d 605, 611 (7th Cir. 2019). The court explained that *Carpenter* "did not invalidate warrantless tower dumps (which identified phones near one location (the victim stores) at one time (during the robberies))." *Id.* at 611.

The defendant's additional *Carpenter*-related arguments do not establish that the government infringed his reasonable expectation of privacy. He argues that Google's information about its users' location is "more precise than the cell site location information at issue in *Carpenter*," ECF No. 29 at 12, but the Supreme Court in *Carpenter* stated that cell-site information "is rapidly approaching GPS-level precision," and *Carpenter*'s holding "t[ook] account of more sophisticated systems that are already in use or in development." *Carpenter*, 138 S. Ct. at 2218-19. Thus, because the Supreme Court grounded *Carpenter*'s holding in an assumption that cell-site information would approach the precision of GPS, any distinction in precision between them

cannot create enhanced Fourth Amendment protections for GPS information.

The defendant also argues that GeoFence information "Allows Law Enforcement to Retrospectively Locate Individuals in Time and Space," ECF No. 29 at 13, but that fact does not distinguish GeoFence information from a wide variety of other business records, or even from witness testimony. For example, credit card records, landline telephone records, employee time sheets, and IP address records may enable law enforcement to retrospectively locate individuals at particular points in time. However, like the GeoFence information, none of these records provide a comprehensive inventory of the whole of a person's movements, and the government does not infringe the privacy interest protected by *Carpenter* when it obtains them. *See, e.g.*, *United States v. Wellbeloved-Stone*, 777 F. App'x 605, 607 (4th Cir. June 13, 2019) (unpublished) (holding that defendant had no reasonable expectation of privacy in IP address information, even after *Carpenter*).

2. The Defendant Has No Reasonable Expectation of Privacy in Location Information He Disclosed to Google

Because *Carpenter* does not create a reasonable expectation of privacy in two hours of location information, Google's disclosure of that information to the United States is subject to the long-standing principle that an individual retains no reasonable expectation of privacy in information revealed to a third party and then disclosed by the third party to the United States. For decades, the Supreme Court has repeatedly invoked this third-party doctrine in cases ranging from private communications to business records, and this principle applies here to the defendant's location information.

For example, in *Hoffa v. United States*, 385 U.S. 293 (1966), the Court applied the third-party doctrine to incriminating statements made in the presence of an informant. The Court held that the Fourth Amendment did not protect "a wrongdoer's misplaced belief that a person to whom

he voluntarily confides his wrongdoing will not reveal it." *Id.* at 302. A decade later the Supreme Court rejected a Fourth Amendment challenge to a subpoena for bank records in *United States v. Miller*, 425 U.S. 435 (1976). The Court held "that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." *Id.* at 443. *See also SEC v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 743 (1984) (applying the third-party doctrine to financial records in the hands of a third-party).

The Supreme Court also relied on this principle in *Smith v. Maryland*, 442 U.S. 735 (1979), when it held that a telephone user had no reasonable expectation of privacy in dialed telephone number information. First, the Court stated that "we doubt that people in general entertain any actual expectation of privacy in the numbers they dial. All telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed." *Id.* at 742. In addition, the Supreme Court further held that even if the defendant had a subjective expectation of privacy in his dialed telephone numbers, "this expectation is not one that society is prepared to recognize as reasonable." *Id.* at 743 (internal quotation marks omitted). The Court explained that the user "voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business." *Id.* at 743-44.

The defendant therefore had no reasonable expectation of privacy in Google's records of his location because he voluntarily conveyed his location to Google in exchange for receiving the benefits of Google services. Because Google location service is an opt-in service, the defendant had previously taken an affirmative step to disclose his location information to Google. Moreover,

he agreed that Google would have access to his location information for purposes ranging from providing him with targeted advertising or assistance with driving directions to Google's development of new services. *See* Google Privacy Policy (available at https://policies.google.com/privacy/archive/20190122). These facts demonstrate that the defendant voluntarily disclosed his location information to Google, and the United States did not infringe his reasonable expectation of privacy when it obtained from Google information about his device's location during a two-hour interval.

Finally, the fact that the defendant voluntarily disclosed his location information to Google is confirmed by the reasoning of *Carpenter*. *Carpenter* concluded that cell-site information was not voluntarily disclosed to the phone company for two reasons, neither applicable here. First, the Court held that carrying a cell phone "is indispensable to participation in modern society." *Carpenter*, 138 S. Ct. at 2220. In contrast, although Google services are frequently helpful and convenient, most may be used without turning on Google location services, and using Google services with location enabled is not essential to participation in modern society. Google location services are no more indispensable than having a bank account or making a phone call, and bank records and dialed telephone number information remain unprotected by the Fourth Amendment under *Miller* and *Smith*. Second, *Carpenter* held that cell-site information is collected "without any affirmative act on the part of the user beyond powering up" and that "there is no way to avoid leaving behind a trail of location data." *Id.* In contrast, in order for Google to have his location information, the defendant had to affirmatively opt in, and he also retained the ability to delete his information. Finally, a cell phone user's disclosure of location information to the phone company is merely incidental to receiving communication service from the company, but a device owner's disclosure of location information to Google is the central prerequisite to obtaining Google

location services. The defendant thus voluntarily disclosed his location information to Google, and Google's disclosure of that information to the government did not infringe upon his reasonable expectation of privacy.

The defendant also asserts that the GeoFence warrant intruded on the reasonable expectation of privacy of others, ECF No. 29 at 13, but this argument fails for two separate reasons. First, the Supreme Court has squarely held that Fourth Amendment rights "may not be vicariously asserted." *Rakas v. Illinois*, 439 U.S. 128, 133-34 (1978) (quoting *Alderman v. United States*, 394 U.S. 165, 174 (1969)). The defendant therefore lacks standing to challenge the government's acquisition of others' location information. *See, e.g.*, *United States v. Patrick*, 842 F.3d 540, 545 (7th Cir. 2016) (rejecting defendant's argument that investigator's use of a cell-site simulator violated the privacy rights of third parties, because the defendant was "not entitled to invoke the rights of anyone else; suppression is proper only if the defendant's own rights have been violated"). Second, these other individuals also voluntarily disclosed their location information to Google. Google's disclosure of their location information therefore did not infringe their Fourth Amendment rights either.

Finally, the defendant claims that obtaining his information from Google constitutes a search under "a property-based theory of the Fourth Amendment." ECF No. 29 at 14. This argument is rooted in Justice Gorsuch's solo dissent in *Carpenter*, where he discussed a transformation of the Fourth Amendment that would jettison not only *Smith* and *Miller*, but also the reasonable expectation of privacy test of *Katz v. United States*, 389 U.S. 347 (1967). *See Carpenter*, 138 S. Ct. at 2262-72 (Gorsuch, J., dissenting). Ultimately, Justice Gorsuch concluded that *Carpenter* forfeited this new argument because he did not raise it below. *See id.* at 2272. Regardless, a solo dissent is not the law, and *Smith*, *Miller*, and *Katz* remain binding on this Court.

Under existing law, Google's disclosure of location information to the government did not infringe upon any reasonable expectation of privacy.

B. The GeoFence Warrant Satisfied the Fourth Amendment

The GeoFence warrant did not remotely resemble a general warrant. A general warrant "specified only an offense—typically seditious libel—and left to the discretion of the executing officials the decision as to which persons should be arrested and which places should be searched." *Steagald v. United States*, 451 U.S. 204, 220 (1981). In contrast, the GeoFence warrant authorized the government to obtain from Google limited and specified information directly tied to a particular robbery at a particular place and time. As set forth below, because the warrant was supported by probable cause and specified its object with particularity, the defendant's argument that the warrant was a general warrant is without merit. *See* ECF No. 29 at 16-24.

More broadly, the facts of this case illustrate why a warrant that requires disclosure of information about devices in a particular place at a particular time is neither a general warrant nor, as the defendant asserts, "repugnant to the Constitution." ECF No. 29 at 16. When law enforcement officers sought the warrant, they were investigating a serious violent crime, and they had reason to believe that the perpetrator was reasonably likely to commit other similar offenses if not identified and apprehended. The GeoFence warrant allowed them to solve the crime and protect the public by examining a remarkably limited and focused set of records from Google: location information over a two-hour interval of three identified and six unidentified individuals, and limited location information over a one-hour interval of ten other unidentified individuals. Rather than being "repugnant to the Constitution," this investigative technique involved no unreasonable search or seizure and should be encouraged, not condemned.

1. The Geofence Affidavit Established Probable Cause

Probable cause requires only "a fair probability, and not a prima facie showing, that contraband or evidence of a crime will be found in a particular place." *United States v. Bosyk*, 933 F.3d 319, 325 (4th Cir. 2019) (quoting *Illinois v. Gates*, 462 U.S. 213, 238 (1983) (internal quotation marks omitted)). It is "not a high bar." *Id.* (quoting *District of Columbia v. Wesby*, 138 S. Ct. 577, 586 (2018). In addition, this Court does not conduct *de novo* review concerning the existence of probable cause: "the duty of a reviewing court is simply to ensure that the magistrate had a substantial basis for concluding that probable cause existed." *United States v. Hodge*, 354 F.3d 305, 309 (4th Cir. 2004) (quoting *Gates*, 462 U.S. at 238–39).

Here, the affidavit in support of the warrant established an ample basis for the issuing magistrate's finding of probable cause. First, it established that an unknown subject committed an armed bank robbery at a particular place and time. *See* State GeoFence Warrant at 4. Second, it established that at the bank prior to the robbery, the robber held the cell phone to his ear and appeared to be speaking with someone. *See id.* Third, the affidavit established that even as of 2013, the majority of cell phones were smartphones. *See id.* at 5. Fourth, it established a connection between smartphones and Google location information. It explained that "[n]early every" Android phone "has an associated Google account," and that Google "collects and retains location data" from such devices when the account owner enables Google location services. *Id.* It also explained that Google can collect location information from non-Android smartphones if the devices are "registered to a Google account and the user has location services enabled." *Id.* From this information, there was a substantial basis for the magistrate to find probable cause to believe that Google possessed evidence related to the robbery.

The defendant objects that there was no probable cause to believe that the bank was robbed by a Google user, *see* ECF No. 29 at 23, but his argument ignores that the probable cause standard requires only a fair probability that evidence will be found at the place searched. The defendant posits a situation in which Google would not have had the robber's location information—"[i]f the robber had an iPhone and did not use Google services"—but he does not dispute that it was likely that Google would have information regarding Android users or that it would have information regarding some non-Android users. ECF No. 29 at 23. The magistrate therefore had a substantial basis for his finding of probable cause.

The United States is unaware of any decisions addressing Fourth Amendment challenges to GeoFence warrants, but one district court recently rejected a similar challenge to cell tower dump warrants. In *United States v. James*, No. 18-cr-216, 2019 WL 325231 (D. Minn. Jan. 25, 2019), the government used tower dump warrants to solve a series of robberies. The defendant there argued that there was no probable cause for the warrants because it was "unknown whether a phone was used by the suspect before or after the robbery." *Id.* at *3. Nevertheless, the district court found that probable cause existed based on the affiant's representations about the "ubiquitous nature" of cell phones, the likelihood of criminals using cell phones, and the storage by cell phone companies of location information. *Id.* Here, where the robber used his phone just before the robbery, the basis for the magistrate's finding of probable cause was at least as strong as in *James*.

Furthermore, the probable cause established by the affidavit supported obtaining Google information for evidentiary purposes other than identifying the robber directly. As the affidavit explained, location information from Google could also "identify potential witnesses" and "assist investigators in forming a fuller geospatial understanding and timeline" of the robbery. State GeoFence Warrant at 5. The warrant appropriately sought such information, as a search warrant

may be issued to obtain evidence to "aid in a particular apprehension or conviction." *Warden v. Hayden*, 387 U.S. 294, 307 (1967).

Messerschmidt v. Millender, 565 U.S. 535 (2012), demonstrates that the Supreme Court does not narrowly construe what may constitute evidence for purposes of a search warrant. In *Messerschmidt*, police obtained a warrant for "all guns and gang-related material" in connection with a known gang member shooting at his ex-girlfriend. *Id.* at 539. In a civil suit under 42 U.S.C. § 1983, Millender challenged the warrant as overbroad, but the Supreme Court rejected the suit based on qualified immunity. *See id.* The Court provided multiple reasons why it was not unreasonable for a warrant to seek "all gang-related materials" in connection with someone shooting at his ex-girlfriend. These reasons included that it could "help to establish motive," that it could be "helpful in impeaching [the shooter]," that it could be helpful in "rebutting various defenses," and that it could "demonstrat[e] [the shooter's] connection to other evidence." *Id.* at 551-52.

Similarly, the issuing magistrate here had multiple reasons to believe that the location information for those present at the robbery would constitute evidence. Investigators could use the location information directly to reconstruct what took place at the crime scene at the time of the crime. They could use it to identify the robber and any accomplices. They could use it to identify potential witnesses and obtain further evidence. They could use it to corroborate and explain other evidence, including surveillance video. They could use it to rebut potential defenses raised by the robber, including an attempt by the robber to blame someone else for his crime. Thus, although the defendant is correct that proximity to criminals does not alone give rise to probable cause that he committed a crime, *see* ECF No. 29 at 21, here probable cause existed for the location information sought by the warrant. The issuing magistrate had a substantial basis for finding

probable cause to believe that Google possessed location information regarding the scene of the robbery, and this Court should therefore deny the defendant's motion to suppress.

Finally, the defendant repeatedly emphasizes that the GeoFence warrant collected information about persons not suspected of criminal activity, but this fact does not aid his Fourth Amendment argument. The Supreme Court has held that "it is untenable to conclude that property may not be searched unless its occupant is reasonably suspected of crime." *Zurcher v. Stanford Daily*, 436 U.S. 547, 559 (1978). Instead, a search warrant "may be issued when it is satisfactorily demonstrated to the magistrate that fruits, instrumentalities, or evidence of crime is located on the premises." *Id.*[4]

2. The GeoFence Warrant Specified its Objects with Particularity

Under the Fourth Amendment, "a valid warrant must particularly describe the place to be searched, and the persons or things to be seized." *United States v. Kimble*, 855 F.3d 604, 610 (4th Cir. 2017) (internal quotation marks omitted). The particularity requirement constrains a warrant so that it is "no broader than the probable cause on which it is based." *United States v. Hurwitz*, 459 F.3d 463, 473 (4th Cir. 2006). It protects against "exploratory rummaging in a person's belongings." *United States v. Williams*, 592 F.3d 511, 519 (4th Cir. 2010) (quoting *Andresen v. Maryland*, 427 U.S. 463, 480 (1976)). Moreover, the test for particularity "is a pragmatic one" that "may necessarily vary according to the circumstances and type of items involved." *United States v. Torch*, 609 F.2d 1088, 1090 (4th Cir. 1979) (quoting *United States v. Davis*, 542 F.2d

[4] *Zurcher*, which approved a warrant to search an innocent newspaper for evidence of crime, also demonstrates that the Fourth Amendment standards of probable cause and particularity govern warrants that raise significant First Amendment concerns. *See id.* at 565 ("courts apply the warrant requirements with particular exactitude when First Amendment interests would be endangered by the search"). Here, the defendant cannot demand any exacting scrutiny of the GeoFence warrant merely because he robbed a bank near a church, because Fourth Amendment rights may not be vicariously asserted. *See Rakas*, 439 U.S. at 133-34. In any event, the GeoFence warrant satisfied the Fourth Amendment under the standards of *Zurcher* because it was issued based on probable cause and specified its objects with particularity.

743, 745 (8th Cir. 1976)).

Here, the GeoFence warrant was narrowly constrained based on location, dates, and times. The warrant sought only location and identity information from Google regarding a two-hour interval for individuals present at the site of a robbery during a one-hour interval. Based on the facts and circumstances investigators knew about the robbery, it was appropriately tailored toward its investigatory purpose, which was to obtain evidence to help identify and convict the armed robber.

The cell tower dump opinion *United States v. James* provides persuasive authority that the warrant here was sufficiently particular. In *James*, the defendant argued that the tower dump warrants used to identify him as a robber were insufficiently particular because they "allowed law enforcement to identify the location of hundreds if not thousands of cell phone users on specific days during specific time frames." *James*, 2019 WL 325231 at *3. The district court, however, found that the warrants were sufficiently particular because they sought information that was "constrained—both geographically and temporally—to the robberies under investigation." *Id.* This reasoning is fully applicable here: the GeoFence warrant was appropriately constrained in space and time to obtain evidence of the robbery. Indeed, the location information obtained from Google was more narrowly constrained than the location information in *James*. The 150-meter radius of the GeoFence warrant is smaller than most cellular sites, and the government only obtained location information regarding 19 individuals, rather than hundreds or thousands.

The defendant also challenges the warrant because it included the three-step process for executing the warrant that allowed investigators to obtain less than the maximum quantity of location and identity information that the warrant authorized. *See* ECF No. 29 at 24 ("The warrant left everything up to the discretion of the executing officers."). The warrant, however, established

probable cause for all the evidence that law enforcement could have obtained: identity information and two hours of location data for all individuals present at the site of the robbery during the hour of the robbery. The information specified by a warrant must be "no broader than the probable cause on which it is based," *Hurwitz*, 459 F.3d at 473, but officers do not violate the Fourth Amendment if they ultimately seize less evidence than the maximum a warrant authorizes. Rather than violating the Fourth Amendment, the three-step process allowed investigators to further protect privacy.

The most-heavily litigated search warrant in history—the search warrant in the investigation of the Playpen child pornography website—included a similar component that allowed investigators to prioritize the evidence they seized, and courts have agreed that that component did not violate the Fourth Amendment.[5] Playpen was a dark web child pornography site with over 158,000 members. *See United States v. McLamb*, 880 F.3d 685, 688 (4th Cir. 2018). FBI investigators obtained a warrant authorizing a search of the computers of everyone who logged into Playpen for 30 days. *See id.* at 689. The attached affidavit, however, allowed the FBI to choose to obtain less than the maximum amount of information the warrant authorized. It explained that that "in executing the requested warrant, the FBI may deploy the NIT more discretely against particular users." *United States v. Anzalone*, 208 F. Supp. 3d 358, 363 (D. Mass. 2016).

[5] Eleven Courts of Appeals have considered various challenges to the Playpen warrant, and all have ultimately rejected suppression. *See United States v. Taylor*, 935 F.3d 1279, 1281 (11th Cir. 2019) ("[W]e become today the eleventh (!) court of appeals to assess the constitutionality of the so-called 'NIT warrant.' Although the ten others haven't all employed the same analysis, they've all reached the same conclusion—namely, that evidence discovered under the NIT warrant need not be suppressed."). Approximately 100 district court cases have resolved suppression motions challenging the Playpen warrant. As discussed in Section III below, the Fourth Circuit rejected a challenge to the particularity of the Playpen warrant based on the good-faith exception. *See United States v. McLamb*, 880 F.3d 685, 689-91 (4th Cir. 2018).

Some defendants argued that the discretion given the FBI in executing the Playpen warrant violated the Fourth Amendment's particularity requirement, but courts uniformly rejected this argument. For example, in *United States v. Matish*, 193 F. Supp. 3d 585, 609 (E.D. Va. 2016), the court concluded that "the fact that the FBI could have and did narrow its search in this case is immaterial, since the warrant was based on probable cause to search any computer logging into the site." *See also Anzalone*, 208 F. Supp. 3d at 368 ("Every court to consider this question has found the NIT search warrant sufficiently particular."). Similarly, the fact that investigators here could have and did narrow the information obtained from Google is immaterial, as the GeoFence warrant was based on probable cause and appropriately authorized seizure of location and identity information of anyone at the site of the robbery. The GeoFence warrant was not a general warrant, and this Court should deny the defendant's motion to suppress.

Finally, even if there were a particularity problem in the three-step process for the GeoFence warrant, the appropriate remedy would at most be to sever the second step of the warrant and to suppress second-step information. "[E]very federal court to consider the issue has adopted the doctrine of severance, whereby valid portions of a warrant are severed from the invalid portions and only materials seized under the authority of the valid portions, or lawfully seized while executing the valid portions, are admissible." *United States v. Sells*, 463 F.3d 1148, 1154–55 (10th Cir. 2006); *see also United States v. Jones*, 2018 WL 935396, at *16–*18 (E.D. Va. Feb. 19, 2014) (discussing and applying doctrine of severance).

Here, the first step of the GeoFence warrant targeted narrow and clearly-defined information: anonymized location information for devices within 150 meters of the bank during the hour of the robbery. Even if this Court were to find the second step to be constitutionally

inadequate, the appropriate remedy would thus be to sever the second step and retain the first.[6] Importantly, first-step information alone was sufficient for investigators to recognize that the Chatrie Account likely belonged to the robber: the defendant's electronic device was near the church prior to the robbery, inside the credit union during the robbery, and left immediately following the robbery via the area near the church. Thus, even if this Court were to sever the warrant and suppress second-step information from Google, the subsequent investigation of the defendant would not be the fruit of the poisonous tree.

C. Evidence from the GeoFence Warrant Should Not Be Suppressed Because Investigators Relied upon it in Good Faith

Even assuming the GeoFence warrant was lacking in probable cause or particularity, suppression would not be an appropriate remedy. Suppression is a remedy of "last resort," to be used for the "sole purpose" of deterring future Fourth Amendment violations, and only when the deterrence benefits of suppression "outweigh its heavy costs." *Davis v. United States*, 564 U.S. 229, 236-37 (2011). "The fact that a Fourth Amendment violation occurred—*i.e.*, that a search or arrest was unreasonable—does not necessarily mean that the exclusionary rule applies." *Herring v. United States*, 555 U.S. 135, 140 (2009). "To trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." *Id.* at 144.

Search warrants for Google information about the location of its users are a new investigative technique, and there are no judicial opinions analyzing them under the Fourth Amendment. In *McLamb*, the Fourth Circuit rejected suppression in this circumstance. The court

[6] Under *Bynum*, 604 F.3d at 164, the defendant lacks a reasonable expectation of privacy in subscriber information obtained under step three of the GeoFence warrant, and he therefore lacks standing to challenge that portion of the warrant.

held that when considering a motion to suppress the fruits of a novel investigative technique, suppression was inappropriate where the investigating officer consulted with counsel and then sought a warrant:

> But in light of rapidly developing technology, there will not always be definitive precedent upon which law enforcement can rely when utilizing cutting edge investigative techniques. In such cases, consultation with government attorneys is precisely what Leon's 'good faith' expects of law enforcement. We are disinclined to conclude that a warrant is 'facially deficient' where the legality of an investigative technique is unclear and law enforcement seeks advice from counsel before applying for the warrant.

McLamb, 880 F.3d at 691. Here, Task Force Officer Hylton followed the approach endorsed by *McLamb*. He had consulted with prosecutors—both state and federal—about GeoFence warrants, and he had previously obtained a similar warrant for Google location information issued by a United States Magistrate Judge. In this investigation, he then sought and obtained a search warrant from a state magistrate. Task Force Officer Hylton thus did "precisely" what *McLamb* expects, and the good-faith exception precludes suppression here.

Alternatively, the traditional good-faith analysis of *United States v. Leon*, 468 U.S. 897 (1984), leads to the same result: no suppression. When police act in "objectively reasonable reliance on a subsequently invalidated search warrant" obtained from a neutral magistrate, "the marginal or nonexistent benefits produced by suppressing evidence … cannot justify the substantial costs of exclusion." *Id.* at 922. *Leon* identified four circumstances in which an officer's reliance on a warrant would not be objectively reasonable:

> (1) when the issuing judge "was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth"; (2) when "the issuing magistrate wholly abandoned his judicial role …"; (3) when "an affidavit [is] so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable"; or (4) when "a warrant [is] so facially deficient—*i.e.*, in failing to particularize the place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be valid."

United States v. Perez, 393 F.3d 457, 461 (4th Cir. 2004) (quoting *Leon*, 468 U.S. at 923). None of these circumstances are present in this case, and the defendant does not claim that the affiant misled the magistrate or that the magistrate abandoned his judicial role.

The defendant argues that the good faith exception does not apply here because the affidavit was so lacking in indicia of probable cause that reliance on it was unreasonable, *see* ECF No. 29 at 24-25, but he is mistaken. As an initial matter, "the threshold for establishing this exception is a high one" because "[o]fficers executing warrants are not often expected to question the conclusions of an issuing authority." *United States v. Seerden*, 916 F.3d 360, 367 (4th Cir. 2019) (quoting *Messerschmidt*, 565 U.S. at 547). The defendant asserts that there was "no evidence that the robber had ever used Google," ECF No. 29 at 24-25, but he ignores that the affidavit established that the armed robber had a cell phone, that most cell phones are smartphones, and that nearly every Android phone user and some non-Android phone users use Google. Based on these facts, the executing officers' belief that the warrant to Google was issued based on probable cause was not entirely unreasonable, and the good faith exception thus precludes suppression.

The defendant also argues that the good faith exception does not apply because the warrant was so facially deficient in failing to specify the things to be seized that officers could not reasonably rely on it. *See* ECF No. 29 at 24. But as discussed in Section II.B above, the warrant was quite specific in scope: it was limited to anonymized location information over a two-hour interval, as well as accompanying identity information for a smaller subset, for individuals present at the site of the robbery during a one-hour interval.

In addition, the defendant argues that the warrant was facially deficient because it allowed officers to choose to obtain less information about those present at the robbery, *see* ECF No. 29 at 25, but this argument is foreclosed by *McLamb*. The defendant in *McLamb* argued to the Fourth

Circuit that the Playpen warrant was insufficiently particular, in part because it allowed the FBI to "deploy the [search technique] more discretely against particular users." *See* Brief of Appellant at 46-47, *United States v. McLamb*, No. 17-4299 (available at 2017 WL 2832704). The Fourth Circuit relied on *Leon*'s good-faith exception to reject suppression, concluding that the Playpen warrant was not "so 'facially deficient ... that the executing officers [could not] reasonably presume it to be valid.'" *McLamb*, 880 F.3d at 691. The warrant thus was not facially deficient, and this Court should deny the defendant's motion to suppress.

III. CONCLUSION

For the reasons set forth in this brief, this Court should deny the defendant's motion to suppress the fruits of the GeoFence warrant.

Respectfully submitted,

G. ZACHARY TERWILLIGER
United States Attorney

By: /s/

Kenneth R. Simon, Jr.
Peter S. Duffey
Assistant United States Attorneys
Office of the United States Attorney
919 E. Main Street, Suite 1900
Richmond, VA 23219
(804) 819-5400
Fax: (804) 771-2316
Email: Kenneth.Simon2@usdoj.gov

Nathan Judish
Senior Counsel, Computer Crime and
Intellectual Property Section
Criminal Division
United States Department of Justice

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on this 19th day of November, 2019, I electronically filed the foregoing with the Clerk of Court using the CM/ECF system, which will send an electronic notification of such filing to the following:

Laura Koenig
Office of the Federal Public Defender (Richmond)
701 E Broad Street
Suite 3600
Richmond, VA 23219
Email: Laura_Koenig@fd.org

Paul Geoffrey Gill
Office of the Federal Public Defender (Richmond)
701 E Broad Street
Suite 3600
Richmond, VA 23219
Email: paul_gill@fd.org

Michael William Price
National Association of Criminal Defense Lawyers
1660 L Street NW
12th Floor
Washington, DC 20036
(202) 465-7615
Email: mprice@nacdl.org
PRO HAC VICE

_____/s/_____
Kenneth R. Simon, Jr.
Assistant United States Attorney
Office of the United States Attorney
919 E. Main Street, Suite 1900
Richmond, VA 23219
(804) 819-5400
Fax: (804) 771-2316
Email: Kenneth.Simon2@usdoj.gov